ANALISA KOMBINASI KUNCI ALGORITMA ELGAMAL MENGGUANAKAN ELLIPTIC CURVE KRIPTOGRAFI

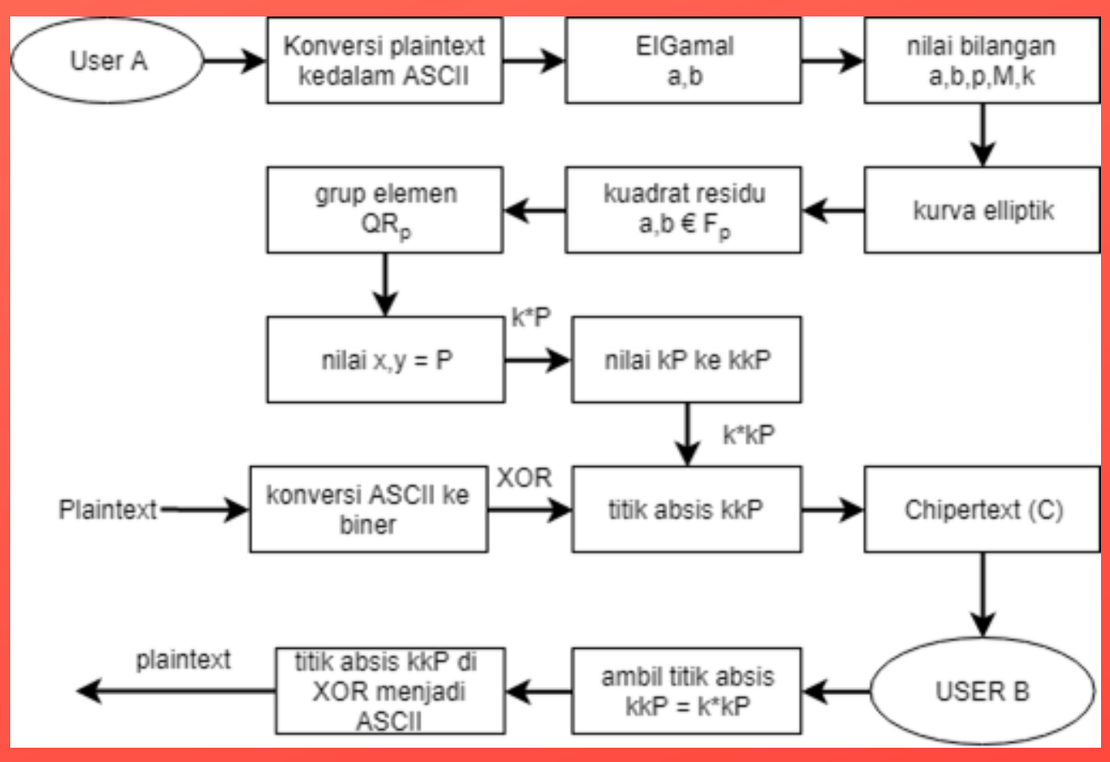
INMAS SETIA BHAKTI
201510370311076

ABSTRAK

Algoritma ElGamal memiliki performa yang lambat dibandingkan dengan algoritma kriptografi simetri yang lainnya. Beberapa penelitian telah dilakukan untuk mengembangkan algoritma ElGamal, namun hasil dari penelitian tersebut membuat performa dari algoritma ElGamal menjadi lebih lambat. Performa waktu rata-rata enkripsi dan dekripsi dengan panjang karakter mulai dari 20 hingga 80 menunjukan bahwa algoritma kombinasi lebih baik dibandingkan algoritma ElGamal. Kekuatan dari algoritma ElGamal dari segi perhitungan diskrit. Algoritma memiliki celah keamanan misalnya, baby-Step giant-step. Penelitian ini menganalisa kombinasi ElGamal dengan Elliptic Curve dengan menggabungkan kekuatan diskrit ElGamal dengan kurva yang akan diimplementasikan pada program berbasis java dan juga menganalisa perbandingan keamanan algoritma ElGamal dan kombinasi ElGamal menggunakan Elliptic Curve dengan menggunakan metode baby-step giant-step. Penelitian ini berhasil menyimpulkan bahwa kombinasi lebih aman daripada ElGamal standar.

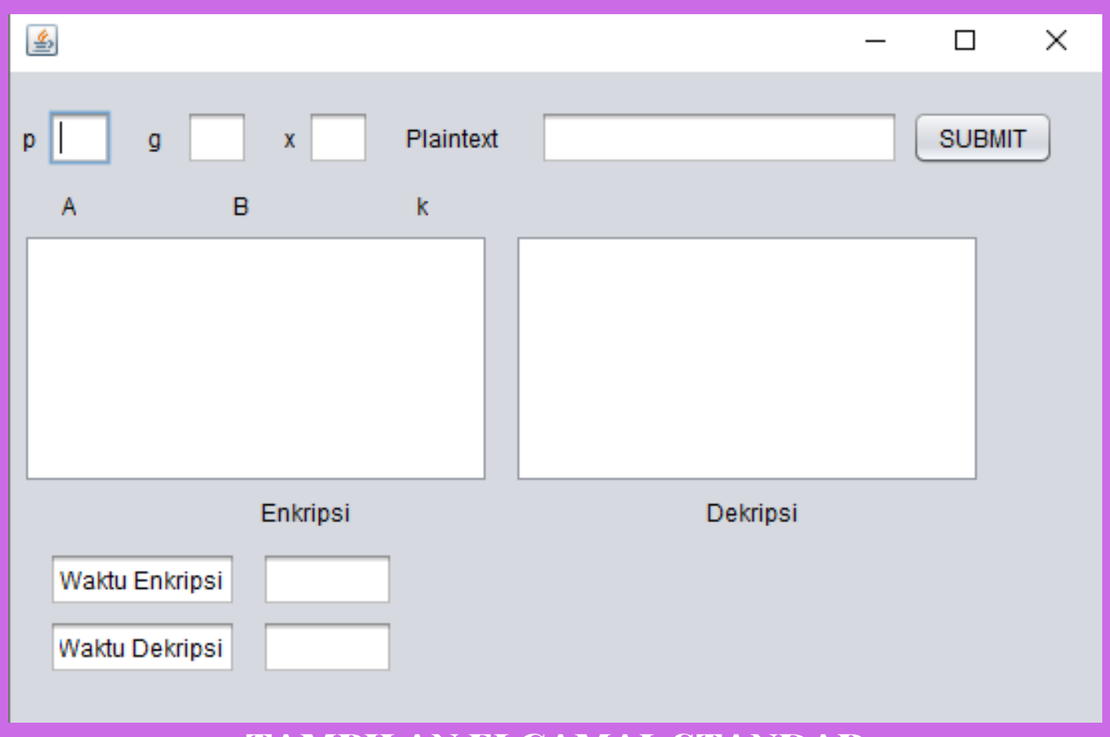
METODE PENELITIAN

1. ElGamal Standar
2. Kombinasi Kunci
3. Elliptic Curve

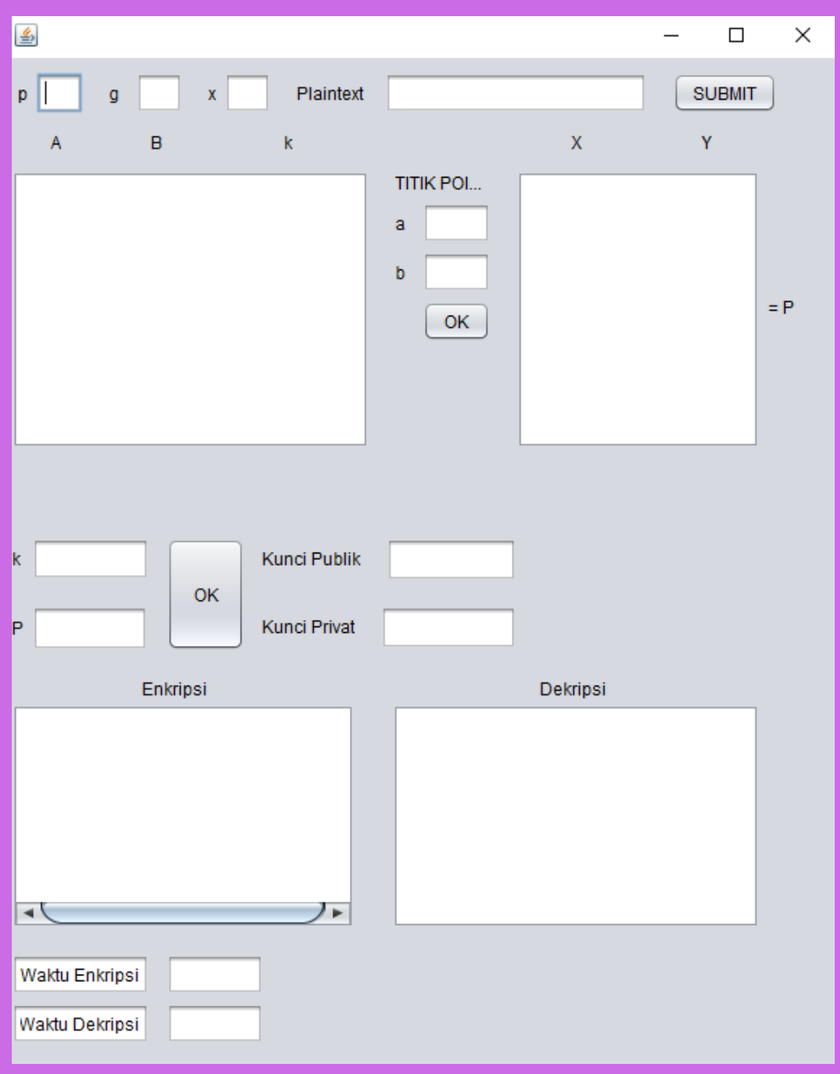


Pengujian

1. **Kombinasi Kunci Algoritma**
   - perhitungan Sistem
2. **Performa**
   - Performa Pembangkitan Kunci
   - Performa Enkripsi
   - Performa Dekripsi
3. **Keamanan**
   - Baby-step Giant-step



TAMPILAN ELGAMAL STANDAR



TAMPILAN KOMBINASI ELGAMAL

KESIMPULAN

1. Algoritma ElGamal dapat di kombinasi dengan Elliptic Curve dan diimplementasikan menggunakan bahasa java.
2. Kombinasi algoritma ElGamal menggunakan Elliptic Curve memiliki performa waktu yang lebih baik dibanding algoritma ElGamal standar pada proses enkripsi dan dekripsi.
3. Kombinasi algoritma ElGamal menggunakan Elliptic Curve lebih aman dibandingkan algoritma ElGamal standar dari serangan menggunakan Baby-step Giant-step.